UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/720,971	04/06/2001	Olli Immonen	367.39437X00	8278

27433 7590 09/08/2006

FOLEY & LARDNER LLP
321 NORTH CLARK STREET
SUITE 2800
CHICAGO, IL 60610-4764

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/720,971	IMMONEN, OLLI	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,15-40 and 42-68* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,15-40 and 42-68* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 09 June 2006 has been entered.

2. By the above submission, Claims 1-5, 15, 19-27, 45-49, and 52-55 have been amended. Claim 14 has been canceled. No new claims have been added. Claims 1-12, 15-40, and 42-68 are currently pending in the present application.

Response to Arguments

3. Applicant's arguments with respect to claims 1-12, 15-40, and 42-68 have been considered but are moot in view of the new ground(s) of rejection.

4. The Examiner notes that, in reference to the Anvret reference (EP 0538216), Applicant argues that Anvret "explicitly teaches against the saving of the master secret code (X)" (page 20 of the present response, emphasis in original). Applicant goes on to

argue that "the specific section cited by the Examiner in the October 31, 2005 Official Action notes that 'by varying X for each session, two sessions will never have the same key'" and to allege that this clearly teaches against saving the master secret code (again, see page 20 of the present response). First, the Examiner notes that the reference to "the specific section cited by the Examiner" is not clear, since at least six excerpts of Anvret were referred to in reference to Claim 1 alone. However, on closer examination, it appears that Applicant is referring to column 7, lines 12-13, of Anvret. Second, the Examiner notes that Anvret was not explicitly relied upon to teach the saving of a master secret code; rather, Ichikawa was relied upon to teach this feature. Third, the Examiner notes that nowhere is it suggested by the Examiner or by Anvret that the variable "X" referred to by Applicant would be considered to be a master secret code; in fact, the portion referred to by Applicant (column 7, lines 12-13) stating that X is changed for each session would itself imply that X is not, in fact, a master key or code. The Examiner further notes that Anvret does disclose storing two variables which remain constant in the system and which are stored on a smart card, namely the variables "a" and "q" which are used in deriving a key (see Anvret, column 5, lines 53-58). Finally, the Examiner believes that the fact that Anvret discloses using a new variable for each session in deriving keys does not preclude the storage of a master secret code; on the contrary, the Examiner notes that Applicant states that keys can be derived based on the master secret and that these derived keys can be used for only a single message before a new key is derived (see page 15, paragraphs 0036-0037 of the

second substitute specification, received 15 August 2005). Therefore, the Examiner believes that Anvret does **not** teach against the storing of a master secret code.

Specification

5. The Examiner thanks Applicant for correcting the errors as noted in the previous Office action(s). However, the objection to the disclosure is NOT withdrawn. The Examiner has noted below several other errors present in the specification. Applicant is respectfully requested to **carefully proofread** the specification and the remainder of the disclosure and correct any other errors that are present. The Examiner has not checked the specification to the extent necessary to determine the presence of **all possible minor errors**. Applicant's cooperation is requested in correcting any other errors of which applicant may become aware in the specification.

6. The disclosure is objected to because of the following informalities:

The specification contains minor typographical, grammatical, or other errors. Note that all page and paragraph references are to the second substitute specification received 15 August 2005, and all line numbers refer to the line number within each paragraph. For example, on page 4, paragraph 0007, lines 4-5, it appears that, in the phrase "This means that the wireless communication apparatus having some kind of contact means", "having" is intended to read "has". On page 5, paragraph 0009, line 2, the phrase "in case of necessary information to re-establishing is saved" is generally

unclear grammatically. Finally, on page 14, paragraph 0034, line 3, it appears that "he" is intended to read "the".

Appropriate correction is required. The above is not intended as an exhaustive list of errors, and Applicant's cooperation is requested in correcting any other errors of which applicant may become aware in the specification.

Claim Objections

7. The objection to Claim 24 is NOT withdrawn. Although Applicant states that the claim has been amended in accordance with the Examiner's suggestion (see page 16 of the present response), it appears that the language in the claim itself has not actually been changed.

8. Claim 24 is objected to because of the following informalities: Claim 24 recites the limitation "at least one a master secret code and at least one signature" in lines 16-17 of the claim. It appears that this is intended to read "at least one of a master secret code and at least one signature".

Appropriate correction is required.

9. The Examiner acknowledges the corrections to the numbering of the claims by the deletion from the record of the duplicate claims 29 and 46, and notes that the application now contains only one claim for each number as required by 37 CFR 1.126.

Claim Rejections - 35 USC § 112

10. The rejection of Claim 14 under 35 U.S.C. 112, second paragraph, is rendered moot in light of the cancellation of the claim.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1, 3-12, 15-19, 21-24, 27-40, 42-44, and 46-68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ichikawa, PCT Publication WO97/24831, in view of Anvret et al, European Publication EP 0538216, and Fang et al, US Patent 6240512.

In reference to Claim 1, Ichikawa discloses a method that includes connecting a wireless communication apparatus to a separate unit; accessing a wireless communication network (page 2, line 16-page 3, line 12); transmitting a request, which includes information on which of at least one algorithm the wireless apparatus supports, from the wireless apparatus to a data communication apparatus (page 10, line 14-page 11, line 11); the data communication apparatus choosing an algorithm and transmitting a message, which includes information about the chosen algorithm, to the wireless

apparatus (page 9, lines 13-23); the wireless apparatus generating a master secret code (page 4, lines 10-12) and calculating a signature based on the chosen algorithm and the master secret code (page 4, lines 12-15); and saving the master secret code on a memory means of the separate unit and in the data communication apparatus (page 7, line 3-page 8, line 4). However, Ichikawa does not explicitly disclose the use of public and private keys.

Anvret discloses a method that includes the use of public and private keys in message communication (column 6, lines 1-11 and 47-48); transmitting a message, which includes the public key, to a wireless communication apparatus (column 6, lines 39-41); transmitting a response, which includes a calculated signature, to a data communication apparatus (column 6, lines 28-41); the data communication apparatus calculating a master secret code based on a chosen algorithm, a received signature, and the private key; and establishing a secure connection between the wireless apparatus and the data communication apparatus (column 6, line 28-column 7, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Ichikawa's method of generating encryption keys with Anvret's method of identification and exchange of encryption keys, in order to promote the usage of smart cards that enable strong algorithms and enhanced security (see Anvret, column 1, lines 23-25).

However, neither Ichikawa nor Anvret explicitly discloses an apparatus generating a master secret code specifically in response to a message. Fang discloses a method in which a master code is generated in response to a message (see column

9, lines 9-15, where master keys are resynchronized in response to initiation by an administrator). Therefore, it would have been obvious to modify the method of Ichikawa and Anvret by including generation of a master code in response to a message, in order to alleviate security concerns, particularly in regard to key exposure (see Fang, column 9, lines 9-11 and 51-53).

In reference to Claim 3, Ichikawa, Anvret, and Fang further disclose re-establishing a connection by transmitting a request, which includes a calculated signature based on the algorithm, public key, and stored secret, from the wireless apparatus to the data communication apparatus (Anvret, column 6, lines 1-11, 39-41, and 47-48). Ichikawa, Anvret, and Fang additionally disclose that the data communication apparatus calculates the master secret code based on the algorithm, signature, and private key, and establishes a secure connection to the wireless apparatus (Anvret, column 6, line 28-column 7, line 13).

In reference to Claim 4 and 27, Ichikawa, Anvret, and Fang further disclose that the separate unit is a smart card (Ichikawa, page 2, lines 16-25; Anvret, column 5, lines 45-58, for example; Fang, column 8, lines 17-25).

Claims 5, 15, 19, 22-24, and 46 each recite limitations recited in, and are substantially equivalent to, Claim 1. The claims are therefore rejected by a similar rationale.

In reference to Claim 6, Ichikawa, Anvret, and Fang further disclose a wireless communication apparatus having an exchangeable memory means (Ichikawa, namely the smart card of page 2, lines 16-25; Anvret, column 2, lines 37-41).

In reference to Claims 7-10, 28-35, 48, 49, and 52-55, Ichikawa, Anvret, and Fang further disclose that the master secret code and signature are each stored and generated on the separate unit (Ichikawa, Figure 1; page 4, lines 2-15).

In reference to Claims 11, 18, 21, 36-40, 43, 44, and 56-64, Ichikawa, Anvret, and Fang further disclose that the separate unit is a smart card (Ichikawa, page 2, lines 16-25; Anvret, column 5, lines 45-58, for example; Fang, column 8, lines 17-25).

In reference to Claims 12 and 65-68, Ichikawa, Anvret, and Fang further disclose that the separate unit is a subscriber identity module (Ichikawa, page 2, lines 16-25).

In reference to Claim 16, Ichikawa, Anvret, and Fang further disclose encryption means for encrypting the master secret (Ichikawa, page 11, line 19-page 12, line 2).

In reference to Claims 17 and 42, Ichikawa, Anvret, and Fang further disclose a secure database including at least one master code or signature (Ichikawa, page 4, lines 12-15; Figure 5; page 7, line 9-page 8, line 10; page 11, line 19-page 12, line 2).

Claim 47 corresponds substantially to Claim 3, and is rejected by a similar rationale.

In reference to Claims 50 and 51, Ichikawa, Anvret, and Fang further disclose a processor generating the master secret code (Ichikawa, page 4, lines 2-15).

13. Claims 2, 20, 25, 26, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ichikawa in view of Anvret and Fang as applied to claims 1 and 19 above, and further in view of Weiss, US Patent 5845519.

In reference to Claims 2 and 20, Ichikawa as modified discloses everything as applied to Claims 1 and 19 above. However, although Ichikawa, Anvret, and Fang disclose changing a master secret (see Fang, column 9, lines 9-11 and 51-53), none of Ichikawa, Anvret, or Fang explicitly discloses saving the master secret for a predefined time. Weiss discloses saving a master key for a predetermined time (column 12, lines 40-61). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of encryption key exchange taught by Ichikawa, Anvret, and Fang with Weiss' teaching of saving keys for a predefined time, in order to prevent an unauthorized user from compromising the key (see Weiss, column 12, lines 40-61).

Claim 25 corresponds substantially to Claim 3, and is rejected by a similar rationale.

In reference to Claims 26 and 45, Ichikawa, Anvret, Fang, and Weiss further disclose that the separate unit is a smart card (Ichikawa, page 2, lines 16-25; Anvret, column 5, lines 45-58, for example; Fang, column 8, lines 17-25).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER